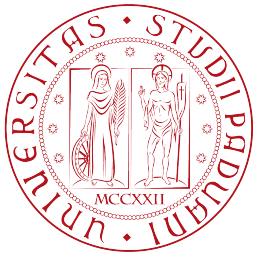
CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Padua@thesis



Università degli studi di Padova

Dipartimento di Fisica e Astronomia

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Fisica

Tesi di Laurea

Distribuzione quantistica di chiavi con metodo Measurement-Device-Independent

Relatore:
Prof. Giuseppe Vallone
Laureando:
Gioele Piccoli

Anno Accademico 2014/2015

Indice

Introduzione

L'obiettivo di questa tesi è introdurre la *distribuzione quantistica di chiavi* (in breve *QKD*), con particolare interesse alla *Measurement-Device-Independent QKD* (*MDI-QKD*), ed ai recenti sviluppi sperimentali di quest'ultima.

Il testo sarà strutturato nel seguente modo: verranno descritti lo scopo e i principi di funzionamento della *QKD*, illustrate le tecniche (strumenti e protocolli) per applicarli, si osserveranno quindi le debolezze dei metodi *standard*, ed infine si descriverà la *MDI-QKD* come possibile soluzione a tali problemi.

Il fine della QKD è distribuire chiavi crittografiche. Queste sono necessarie per applicare la *crittografia*. Lo scopo della crittografia è rendere segreto un messaggio, in modo che due utenti possano comunicare senza che altri riescano a conoscere l'informazione.

Per ottenere una comunicazione segreta è necessario cifrare il messaggio. Algoritmi per questa operazione sono stati sviluppati nel corso della storia, ma tutti necessitano di una chiave per codificare e decodificare il messaggio stesso. Il problema si focalizza, quindi, su come scambiare segretamente una chiave.

I metodi classici trasmettono la chiave sullo stesso canale su cui si trasmetterà il messaggio. Le tecniche di trasmissione sono tali per cui un infiltrato, che volesse conoscere la chiave, dovrebbe impiegare un'ingente potenza di calcolo per un lungo intervallo di tempo prima di ricavarla. In questo modo quando egli trovasse la chiave, l'informazione decriptata sarebbe ormai vecchia e dunque inutile. Tuttavia non si può escludere a priori che venga sviluppato un dispositivo di maggiore velocità, che permetta di rubare la chiave in tempi rapidi.

La QKD, al contrario, sfrutta principi della Meccanica Quantistica per dare la certezza che l'intruso non possa conoscere la chiave, indipendentemente dai dispositivi utilizzati. Cosa possibile in quanto le leggi fisiche permettono di conoscere se c'è stata un'intrusione e quali informazioni sulla chiave sono state rubate.

Capitolo 1

Quantum Key Distribution

Lo scopo primo della *Quantum Key Distribution* (QKD), come suggerisce il nome, è distribuire a due (o più) utenti una *chiave* crittografica segreta, che consiste in una sequenza di bit. Questa chiave potrà poi essere utilizzata dai due per qualunque operazione necessiti di essa, per esempio: la criptatura di dati, l'autenticazione a servizi online, ecc... La necessità fondamentale del processo è che la chiave sia segreta, ossia nota solo ai due utenti e non disponibile ad un eventuale malfattore.

I metodi classici utilizzati per distribuire chiavi segrete basano la loro sicurezza sulla capacità di calcolo dell'avversario. Ossia è teoricamente possibile rubare queste chiavi durante la trasmissione senza essere scoperti, ma il tempo che si impiegherebbe per farlo è talmente tanto che una volta trovata sarebbe ormai inutile. La maggiore insidia a questa tecnica tradizionale è la creazione dei computer quantistici. Infatti il tempo necessario a rubare la chiave è molto elevato per computer classici, ma le stesse operazioni sarebbero eseguite in tempi drasticamente minori da quelli quantistici, rendendo totalmente non sicure le chiavi.

La *QKD* basa invece la sua sicurezza su *leggi fisiche* della meccanica quantistica. Queste ultime permettono di sapere se sono stati rubati dati durante lo scambio, e in tal caso le informazioni compromesse vengono cancellate. Si avrà dunque la sicurezza che la chiave scambiata è segreta e non può essere stata rubata, indipendentemente dalle capacità dell'avversario.

Facciamo una precisazione sul significato della sicurezza: nessuna chiave è sicura in senso assoluto. Questo perché un malintenzionato potrebbe o indovinare la chiave casualmente o con un cosiddetto attacco *Brute-Force*(nel quale un sistema prova tutte le possibili combinazioni di bit della chiave). Quello che è importante per la *QKD* è la *sicurezza incondizionata*. Questo significa che la segretezza della chiave è garantita indipendentemente dalla potenza di calcolo dell'avversario. La chiave, perciò, non può essere rubata ma non è sicura in senso assoluto.

Introduciamo brevemente alla terminologia che verrà frequentemente utilizzata in seguito. Verranno chiamati *Alice* e *Bob* le due parti che alla fine dovranno condividere la chiave segreta, *Eve* (da *eavesdropper*, ladro/origliatore) colei che cercherà di rubare la stessa chiave senza farsi scoprire, e *Charlie* un terzo utente, quando necessario.

1.1 Generazione della chiave

Il metodo utilizzato per generare e scambiare la chiave si divide in diversi step. Come prima cosa dei *qubit* vengono scambiati su un canale quantistico; in questo canale un'intromissione di Eve comporta necessariamente una modifica dei segnali trasmessi, quindi può essere individuata. I qubit vengono prodotti e identificati con diversi protocolli, che illustreremo in seguito. Dopo questa fase Alice e Bob hanno a disposizione ciascuno una sequenza di bit detta *raw key*, ma le due non sono necessariamente perfettamente correlate. Si procede dunque ad una post-

elaborazione eseguita su un canale classico autenticato: questo canale è pubblico ed Eve può sapere tutto quello che viene detto, ma non può interagire; in particolare non può fingere di essere Alice o Bob poiché è necessaria un'autenticazione (che deve essere sicura). La post-elaborazione si distingue ulteriormente in due procedimenti: la *correzione degli errori* (EC) e la *amplificazione della privacy* (PA).

1.1.1 Informazione quantistica

Il primo passo nella creazione della chiave è lo scambio di informazioni su un canale quantistico. Generalmente (ma non sempre) sarà Alice a preparare uno stato quantistico $|\Psi(S_n)\rangle$, dove la corrispondente sequenza S_n è definita dal protocollo utilizzato. Il ruolo di Bob sarà eseguire le misure per decodificare il segnale e valutare la perdita di informazione nello scambio, attribuibile ad un'intromissione di Eve.

Questo tipo di schema è stato nei primi anni il più utilizzato, poiché di più semplice implementazione, e viene chiamato *prepare-and-measure* (P&M). Un altro schema proposto è quello *entanglement-based* (EB): in questo caso Alice prepara uno stato entangled, effettua una misura nella sua base e invia a Bob un segnale corrispondente a quanto misurato. Una terza possibilità, che tratteremo più a fondo in seguito, è il *measurement-device-independent*, in cui sia Alice che Bob generano uno stato e lo inviano a Charlie, il quale è l'unico ad effettuare misure.

La QKD può essere sviluppata con qualunque sistema quantistico. Tuttavia, essendo richiesta la trasmissione su lunghe distanze, la scelta è storicamente caduta sul *fotone*. La luce infatti interagisce poco con la materia e questo permette una trasmissione veloce e senza un'eccessiva distorsione del segnale.

Come sorgente si utilizzano generalmente *LASER* attenuati, in cui la probabilità di produrre n fotoni in un segnale è data da

$$P(n|\mu) = e^{-\mu}\mu^n/n! \tag{1.1}$$

dove μ è l'intensità (o numero medio di fotoni) del Laser. Il segnale viene quindi modificato da modulatori di fase, amplificatori-attenuatori e polarizzatori, quindi inviato a Bob.

Il trasferimento del fotone viene eseguito principalmente su due canali: via aria, o via fibra ottica. Il primo necessita di una linea di vista tra Alice e Bob; ha il vantaggio di produrre una decoerenza del segnale del tutto trascurabile e lo svantaggio di introdurre perdite di tipo geometrico (dovute all'apertura dei telescopi che inviano e ricevono il segnale) e atmosferico. Il secondo risente anch'esso di perdite, con una trasmittività.

$$t = 10^{-\alpha l/10} \tag{1.2}$$

dove α dipende dalla lunghezza d'onda del segnale, ed i valori ottimali sono dell'ordine di $\alpha \simeq 0.3 dB/km$.

Infine la rivelazione viene fatta con dei contatori di fotoni, che consistono in strumenti i quali danno un *click* quando vengono colpiti da un fotone. Le caratteristiche dei rivelatori sono: l'efficienza η, ossia la probabilità che un fotone sia rivelato, e il tasso di *dark count* p_d, la frequenza di false rivelazioni.

La stima del qubit viene fatta con metodi differenti in relazione al protocollo utilizzato(vedi sezione 1.2), in particolare la misura sul fotone varia a seconda del grado di libertà scelto per la codifica. In generale nell'apparato di misura sono presenti più rivelatori intermediati da ulteriori strumenti (beam-splitter, inferferometri, polarizzatori, ecc...). Questi ultimi ricevono il fotone e lo inviano ad uno specifico rivelatore in base allo stato del fotone stesso. Il click di uno (o più) dei rivelatori corrisponderà ad un determinato risultato della misura.

Facciamo un esempio concreto, in caso di codifica nella polarizzazione. L'apparato di misura di Bob sarà composto da un beam-splitter polarizzatore (PBS) collegato a tre linee ottiche: un ingresso (proveniente da Alice) e due uscite, ciascuna delle quali termina in un rivelatore (D1, D2). Un fotone inviato da Alice raggiunge il PBS, che lo trasmette in una delle due uscite a seconda dello stato di polarizzazione, raggiungendo solo uno tra D1 e D2. In questo modo il click di D1 corrisponde a $|+\rangle$ mentre D2 a $|-\rangle$, autostati di polarizzazione nella base del PBS. Lo stato di un fotone è dunque identificato, da Bob, in modo univoco se uno e uno solo dei due rivelatori rivela il fotone stesso. Successivamente Alice e Bob dovranno verificare se le basi di generazione e misura della polarizzazione fossero parallele o meno.

1.1.2 Informazione classica

Dopo lo scambio di segnali sul canale quantistico Alice e Bob hanno ciascuno una lista di N bit, e devono praticare un'analisi su questi sfruttando il canale classico. In alcuni protocolli la prima fase è il *sifting*: Alice e Bob decidono di scartare alcuni bit, nei quali il procedimento di codifica è stato errato (per esempio produzione e misura sono state fatte con basi diverse). Successivamente viene eseguita la *stima dei parametri*: con studi statistici si valutano i parametri del canale quantistico come trasmittività, tasso di errore e tasso di rivelazione. A questo punto Bob e Alice possiedono una sequenza di $n \leq N$ bit, detta *Raw Key*.

La fase successiva è la generazione della chiave segreta a partire dalla Raw Key. Come prima cosa viene eseguita una correzione degli errori, e successivamente la amplificazione della privacy. Quest'ultima è fondamentale perché consiste nel valutare quante informazioni sono potenzialmente note ad Eve, le quali vengono rimosse dalla chiave. Al termine della procedura si avrà una sequenza, condivisa da Alice e Bob, di $L \leq n$ bit, la *Secure Key*.

Si definiscono delle quantità per la stima dell'efficienza dei protocolli utilizzati. Nel caso asintotico di chiave infinita, la *frazione segreta*

$$r = \lim_{N \to \infty} L/n \tag{1.3}$$

che indica la dimensione della Secure Key che si può ottenere dalla Raw Key. Sperimentalmente è utile definire la *secure key rate*

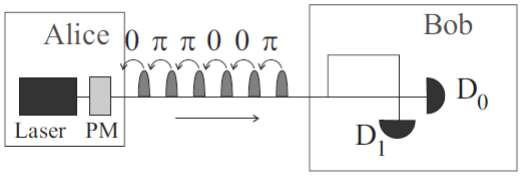
$$R = L/N \tag{1.4}$$

ossia il rapporto tra la lunghezza (numero di bit) L della chiave segreta e il numero di segnali N scambiati per produrla.

1.2 Protocolli

I protocolli consistono in un insieme di istruzioni per Alice e Bob, descriventi i procedimenti di produzione e misura del segnale quantistico, e la successiva post-elaborazione. Si distinguono principalmente tre famiglie di protocolli: *discrete-variable* coding, *continuos-variable* coding, *distributed-phase-reference* coding. La codifica a variabili discrete è quella maggiormente diffusa nelle implementazioni e affronteremo di essa due protocolli (1.2.1 BB84 e 1.2.2 SARG04); vedremo infine un esempio di codifica in fase (1.2.3 DPS), e un protocollo alternativo (1.2.4 COW).

Figura 1.1: Differential phase shift protocol. Legenda: PM modulatore di fase.



1.2.1 BB84

Il protocollo *BB84* (*Bennet and Brassard, 1984*) è stato il primo proposto ed è a variabile discreta. Alice prepara una particella singola in uno dei quattro stati:

$$|+x\rangle, |-x\rangle, |+y\rangle, |-y\rangle \tag{1.5}$$

autostati degli operatori di Pauli σ_x, σ_y. Gli stati + codificano con il valore 0 del bit, mentre gli stati − con 1. Bob misura casualmente su una delle due basi. Si procede successivamente al *sifting*: Alice rivela la base utilizzata su ciascun segnale, entrambi accettano solo gli eventi in cui hanno utilizzato la stessa base e scartano gli altri.

La sicurezza incondizionata di questo protocollo è stata dimostrata [1, page 1312].

1.2.2 SARG04

Il protocollo *SARG04* (*Acín, Gisin, and Scarani, 2004; Scarani, Acín, Ribordy, and Gisin, 2004*) è un'evoluzione del precedente. Usa le stesse basi ma i bit sono codificati sulle basi e non sugli stati: base X corrisponde a 0 e Y a 1. Come prima Alice genera il segnale e Bob lo misura, utilizzando le due basi con la stessa probabilità 1/2. Quindi Bob annuncia il risultato della sua misura s_B e Alice replica di accettare solo se lei ha preparato lo stato opposto $s_A = -s_B$. In caso positivo Bob effettua un *bit-flip*: si segna il valore opposto a quello della base utilizzata. Facciamo un esempio: Alice invia $|+y\rangle$, se Bob misura Y ottiene +, se misura X ottiene con ugual probabilità + o −; è evidente che si ha una corrispondenza univoca solo se Bob misura − e questo significa che ha sbagliato base, che dunque inverte con il *bit flip*.

Questo protocollo è meno efficiente del precedente in quanto tendenzialmente scarta un numero maggiore di segnali durante il *sifting*, ma è stato inventato poiché nell'implementazione con laser attenuati (sorgenti non a particella singola) è più resistente agli attacchi di *photon number splitting* (PNS).

1.2.3 DPS

Il *differential phase shift* è stato il primo protocollo ideato con codifica in fase. Alice produce una sequenza di stati coerenti con uguale intensità

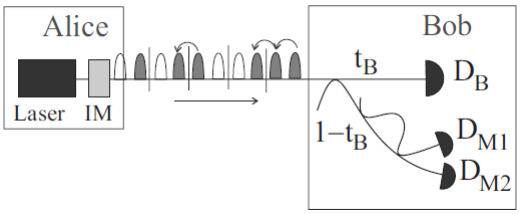
$$|\Psi(S_n)\rangle = \cdots |e^{i\varphi_{k-1}}\sqrt{\mu}\rangle |e^{i\varphi_k}\sqrt{\mu}\rangle |e^{i\varphi_{k+1}}\sqrt{\mu}\rangle \cdots \tag{1.6}$$

dove le fasi possono assumere i valori $\varphi = 0$ e $\varphi = \pi$ (figura 1.1). I bit sono codificati dalla differenza di fase tra due segnali successivi: $bit_k = 0$ se $\phi_k = \phi_{k+1}$, $bit_k = 1$ altrimenti.

1.2.4 COW

Facciamo infine un cenno al protocollo *coherent one way*, che non rientra nelle categorie precedenti. In questo i bit sono codificati con sequenze di segnali di intensità μ e segnali vuoti (fig.

Figura 1.2: Coherent one way protocol. Legenda: IM modulatore di intensità.



1.2), in questo modo: $bit_k = 0$ con la sequenza $|\sqrt{\mu}\rangle_{2k-1}|0\rangle_{2k}$, $bit_k = 1$ con $|0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$. Dove gli stati vuoti sono identificati misurando gli intervalli di arrivo degli stati non vuoti.

L'analisi, per valutare i parametri della comunicazione, si esegue solo nei casi di due impulsi non vuoti consecutivi. Questi casi si verificano normalmente quando viene codificata la sequenza 10, oppure possono essere prodotti appositamente per il controllo.

Nei protocolli *DPS* e *COW* il segnale inviato non è scrivibile come prodotto tensore di singoli stati, perché gli stati successivi sono correlati; per esempio nel DPS lo stato $k-esimo$ codifica sia il bit k che il bit $k-1$. A causa di questo non è ancora stata dimostrata la sicurezza incondizionata per tali protocolli, poiché tutte le attuali dimostrazioni si basano sulla scomposizione del segnale.

Capitolo 2

Sicurezza ed attacchi

In questo capitolo daremo una breve nozione sulle tecniche per ottenere una chiave sicura, in particolare sui parametri di generazione della stessa. Vedremo di seguito dei possibili attacchi ad un apparato pratico e le relative conseguenze sulla sicurezza.

Nella trattazione della sicurezza lavoreremo in *uncalibrated-device scenario* [1, page 1325]: ogni perdita di dati nella comunicazione ed ogni errore sono attribuiti ad un'informazione disponibile ad Eve. Questa condizione è ovviamente pessimistica, in quanto perdite nella linea ed errori di rivelazione esistono e possono essere stimati; ad oggi però la sicurezza incondizionata è stata dimostrata solo in questo scenario.

Introduciamo qui il formalismo per i parametri utilizzati di seguito, per quanto riguarda la produzione della chiave. Si definiscono: il tasso di rivelazione per un impulso di n fotoni R_n; il tasso totale di rivelazione $R_T = \sum_n R_n$; lo *yield* $Y_n = R_n/R_T$; il tasso d'errore su un segnale di n fotoni $e_n = R_n^w/R_n$, dove R_n^w è la frazione di errori in R_n; il tasso d'errore totale ($QBER$) $E = \sum_n Y_n e_n$; il gain $Q_n = Y_n p_n$, dove p_n è la probabilità di produrre un impulso da n fotoni (vedi eq 1.1).

Una possibile strategia di Eve è il cosiddetto attacco *intercept-resend*: Eve intercetta il fotone di Alice, fa una misura, e invia a Bob un fotone corrispondente al risultato della misura effettuata. Eve sceglie la base di misura in modo casuale, avrà in media un'informazione esatta su metà dei segnali: $I_E = 0.5$, introducendo però un errore sulle misure di Bob pari a $E = 0.25$ (ossia metà dei casi in cui Eve usa la base sbagliata). Il quesito della QKD a questo punto è se una chiave sicura può essere estratta in presenza di tale $QBER$. Sotto determinate assunzioni si trova [1]

$$r = max\{I(A:B) - I_E, 0\} \tag{2.1}$$

dove $I(A:B)$, l'informazione reciproca tra le chiavi di Alice e Bob, può essere riscritta (se i valori dei bit sono equiprobabili) $I(A:B) = 1 - H(E)$, con H entropia binaria. Si verifica dunque che non è possibile ricavare una chiave sicura ($r = 0$) in quanto l'informazione che ha Eve sulla chiave di Bob è maggiore di quella di Alice. Più dettagliatamente si può trovare che non è possibile ricavare una chiave se l'attacco *intercept-resend* è effettuato su più del 68% dei fotoni.

Cerchiamo ora di ottenere una formula per il secure key rate ottenibile in un'applicazione sperimentale. In generale la *secret key fraction* si può scrivere [1]

$$r = I(A:B) - min(I_{EA}, I_{EB}) \tag{2.2}$$

dove $I(A:B)$ è l'informazione reciproca tra Alice e Bob e I_{EA} e I_{EB} sono l'informazione che ha Eve sulle chiavi di Alice e Bob, rispettivamente.

Nello specifico caso dei protocolli a variabile discreta, si può semplificare 2.2 come

$$r = 1 - leak_{EC}(E) - I_E \tag{2.3}$$

dove $leak_{EC}(E) \geq H(E)$ e $I_E = min(I_{EA}, I_{EB})$.

Per i vari protocolli sarà dunque necessario calcolare E e stimare I_E per conoscere il tasso di generazione della chiave segreta. Il primo parametro può essere ricavato da una semplice analisi statistica, mentre il secondo presenta i maggiori problemi. Si può dimostrare che [1]

$$I_E = \max_{Eve} \sum_n Y_n I_{E,n} \tag{2.4}$$

dove il massimo è calcolato su tutti i possibili attacchi di Eve. Per un protocollo a variabile discreta segue che [1]

$$I_E = 1 - \min_{Eve}\{Y_0 + Y_1[1 - H(e_1)]\}. \tag{2.5}$$

A questo punto è necessario individuare la condizione ottimale per Eve. Questa si ottiene trovando il minimo di Y_1 ed il massimo di e_1.

In un approccio *standard* i soli parametri misurati sono R_T ed E; per cui è necessario supporre $e_{n\geq 2} = 0$, ottenendo quindi $e_1 = E/Y_1$. Di conseguenza l'attacco ottimale di Eve è quello che minimizza Y_1; questo si ottiene massimizzando il numero di impulsi a multifotone ($n_{fotoni} \geq 2$) inviati da Alice. In questo modo si ottiene un limite alla frazione sicura [1]

$$r \geq Y_0 + Y_1[1 - h(E/Y_1)] - leak_{EC}(E) \tag{2.6}$$

dove $Y_1 \geq Y_1^{low}$, essendo quest ultimo il minimo descritto.

La debolezza di questo approccio consiste nel fatto di disporre di pochi dati sperimentali, per cui le stime sull'informazione di Eve risultano essere eccessivamente ottimistiche. Per migliorare questo risultato viene ideata la tecnica *decoy states*.

2.1 Decoy States

La tecnica a stati decoy si applica nel seguente modo: durante lo scambio dell'informazione sul canale quantistico, Alice varia casualmente un parametro ξ del segnale (generalmente l'intensità del Laser). In questo modo Eve non può ottimizzare il suo attacco sul tipo di segnale, perché non lo conosce. Ultimato lo scambio Alice comunica pubblicamente la lista dei valori assunti da ξ e l'analisi, con Bob, viene fatta separatamente per ogni valore.

Nell'ipotesi che il parametro modificato sia l'intensità del laser, denotiamo con μ l'intensità degli impulsi di segnale e con ν_i l'intensità degli impulsi del i-esimo stato decoy utilizzato.

L'analisi statistica permette quindi di avere un maggior numero di equazioni, due per ogni stato decoy

$$Q_{\nu_i} = \sum_k Y_k \frac{\nu_i^k}{k!} e^{-\nu_i} \tag{2.7}$$

$$E_{\nu_i} Q_{\nu_i} = \sum_k e_k Y_k \frac{\nu_i^k}{k!} e^{-\nu_i} \tag{2.8}$$

oltre a quelle per gli impulsi di segnale.

L'obbiettivo della tecnica a stati decoy è utilizzare queste informazioni per avere una miglior stima sull'informazione di Eve (eq. 2.5) e, quindi, un migliore secure key rate. Per fare questo è necessario stimare il minimo di Y_1 ed il massimo di e_1.

Si osserva che per ottenere questi due limiti sono sufficienti due stati decoy. Consideriamo dunque ν_1 e ν_2 tali che $0 \leq \nu_2 \leq \nu_1$ e $\nu_1 + \nu_2 < \mu$. In queste condizioni, utilizzando le eq. 2.7 e 2.8 si trovano [2] il limite inferiore di Y_1

$$Y_1^{L,\nu_1,\nu_2} = \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}(Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)) \tag{2.9}$$

dove

$$Y_0^L = \max[\frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0]$$

e il limite superiore di e_1

$$e_1^{U,\nu_1,\nu_2} = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^{L,\nu_1,\nu_2}} \tag{2.10}$$

dove E_* e Q_* sono misurati sperimentalmente.

Si può osservare [2] che i limiti trovati tendono ai valori ideali, ottenibili con un numero infinito di stati decoy, se $\nu_1 \to 0$ e $\nu_2 \to 0$. In particolare: minore è la quantità $\nu_1 + \nu_2$, migliore è la stima dei parametri, maggiore è il secure key rate.

Nasce dunque spontanea l'idea di un protocollo con due stati decoy, di cui uno ad intensità nulla (vuoto). Lo stato vuoto fornisce direttamente le stime $Q_{vuoto} = Y_0$ e $E_{vuoto} = e_0 = 1/2$, quest'ultimo in virtù del fatto che i dark counts avvengono casualmente. In tale situazione, con $\nu_2 = 0$, le precedenti eq. 2.9 ed eq. 2.10 si semplificano

$$Y_1^{L,\nu,0} = \frac{\mu}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \tag{2.11}$$

$$e_1^{U,\nu,0} = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{\nu Y_1^{L,\nu,0}}. \tag{2.12}$$

La tecnica a stati decoy permette dunque di ottenere un miglior secret key rate, in quanto si può stimare in modo ottimale l'informazione di Eve, senza sovrastimarla come avveniva con l'approccio senza stati decoy.

Sono stati mostrati dunque i limiti della velocità di produzione di una chiave sicura, in caso di perdita di informazioni (attribuita ad un attacco di Eve). Gli attacchi considerati sin qui sono però fondati su un apparato ideale. Gli apparati reali presentano ulteriori debolezze, basate sulla non-idealità dei componenti, che possono essere sfruttate da Eve senza essere, potenzialmente, scoperta. Queste falle riguardano il funzionamento degli strumenti, in particolare il lato più debole sembra essere quello di rivelazione. Infatti esso è costantemente in *fase di lettura* e Eve può mandargli qualunque tipo di informazione. Nel seguente paragrafo vedremo un esempio di attacco ad un apparato reale.

2.2 Attacco a sistema QKD

Lydersen [3] ha illustrato una falla in due sistemi commerciali di *QKD*, e dimostrato come sia relativamente semplice acquisire la chiave segreta mediante l'utilizzo di una particolare sorgente luminosa.

Molti sistemi QKD utilizzano come rivelatori degli *APD* (*avalanche photodiodes*) in modalità *Geiger*; per mantenere questa modalità il rivelatore deve essere mantenuto ad un potenziale maggiore del potenziale di breakdown V_{br}, al di sotto del quale funziona diversamente: in modalità *lineare* (fig. 2.1). Tuttavia per evitare un tasso eccessivo di dark counts, i rivelatori vengono tenuti ad una tensione costante $V_{bias} < V_{br}$ e passano in modalità Geiger solo quando è atteso l'arrivo di un fotone (fig. 2.2). Quando il rivelatore si trova in modalità lineare esso è vulnerabile ad un attacco tramite un'apposita illuminazione dello stesso. In questa modalità il click viene dato quando il segnale in ingresso supera una certa soglia P_{th}. Eve effettua un attacco *intercept-resend*: intercetta il fotone di Alice, lo misura, e invia degli impulsi luminosi (non un singolo fotone) con potenza di poco superiore a P_{th}. In questo modo se Bob sta utilizzando la stessa base di Eve, il rivelatore clicca ed i due hanno la stessa informazione; se invece sta usando una base differente il fascio viene diviso in due di potenza dimezzata, e i rivelatori non

Figura 2.1: Funzionamento APD (Avalanche photodiode). In modalità Geiger, un singolo fotone assorbito produce una grande corrente I_{APD} attraverso il contatore; il rivelatore clicca quando la corrente supera una soglia I_{th}. In modalità lineare la corrente I_{APD} è proporzionale alla potenza del segnale in ingresso; quindi una potenza maggiore di P_{th} fa cliccare il contatore, in quanto produce una corrente maggiore della soglia.

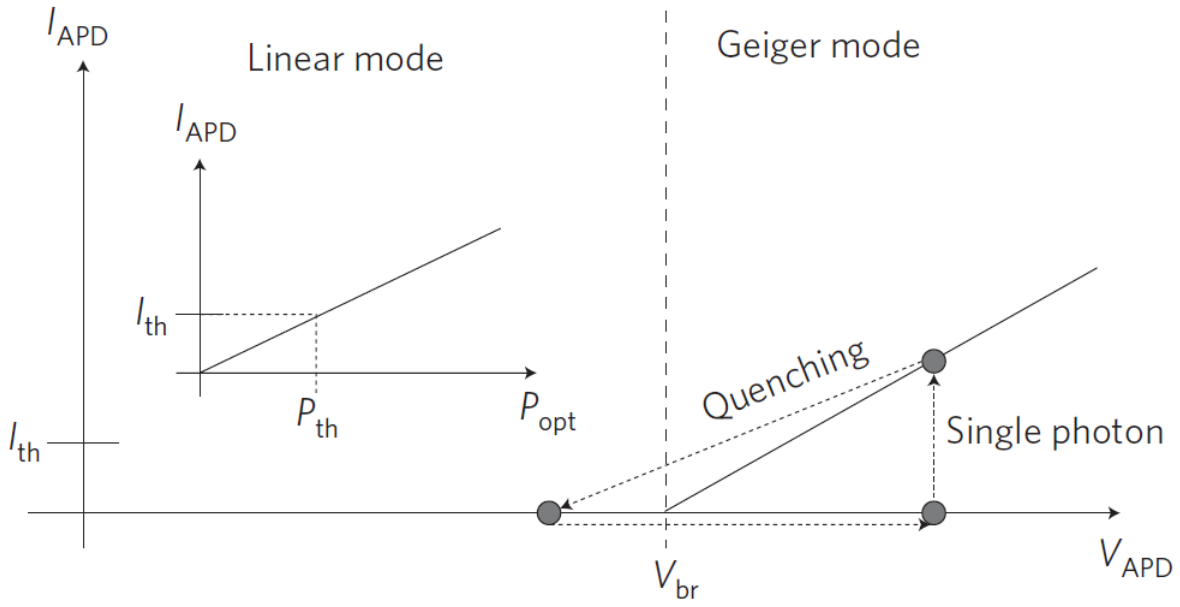


Figura 2.2: Potenziale APD. L'APD è portato in modalità Geiger solo quando si attende l'arrivo di un fotone. Praticamente il fotodiodo è mantenuto ad un potenziale minore di quello di breakdown, e periodicamente un impulso elettrico lo porta in modalità Geiger

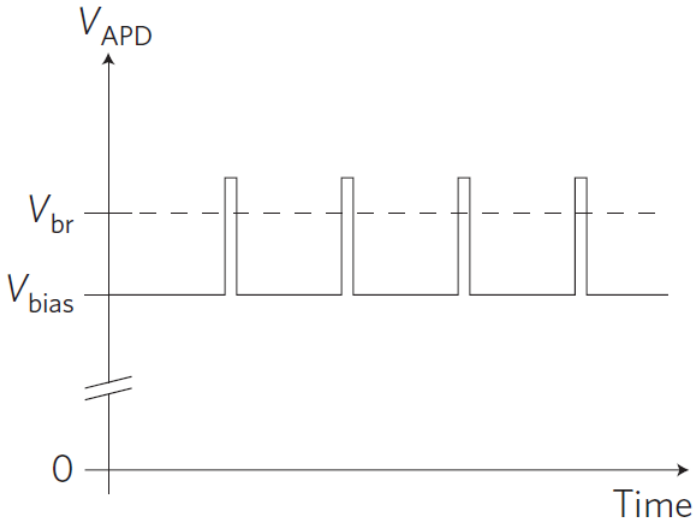
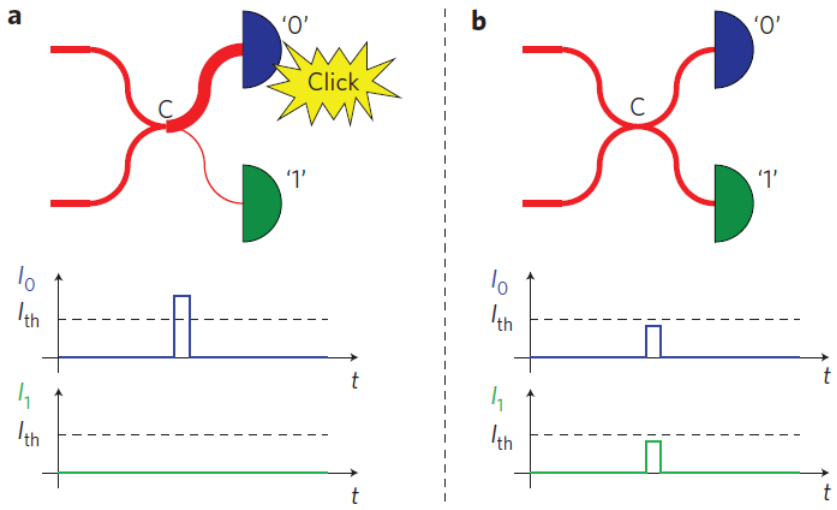


Figura 2.3: Segnali di Eve a Bob. **a**, se Eve e Bob usano la stessa base, i due fasci interferiscono costruttivamente e producono sul detector opportuno un click. **b**, se invece usano basi diverse, i due impulsi non si uniscono e non producono click in nessun rivelatore.



cliccano (fig. 2.3). In alternativa Eve può inviare un segnale di potenza superiore al doppio di P_{th}, in modo che ad uguali basi corrisponda un click ma a basi diverse corrisponda un doppio click (che rappresenta un errore per Bob). Alla fine dello scambio Eve e Bob hanno le stesse informazioni, Eve segue poi le stesse procedure di Bob per la correzione errori e l'amplificazione della privacy, ottenendo una copia esatta della chiave segreta senza essere scoperta.

Questo attacco è molto generico e può essere applicato a moltissimi dispositivi QKD, ma in futuro si potrebbero trovare delle contromisure. Per esempio la potenza di soglia P_{th} non è una quantità esatta, ma anzi si possono definire P_{sempre} sopra la quale il rivelatore clicca sempre, e P_{mai} sotto la quale non clicca. Dato un sistema con più rivelatori, si trova che l'attacco è possibile solo se vale [3]

$$\max_i[P_{sempre,i}] < 2(\min_i[P_{mai,i}]) \tag{2.13}$$

dove i indica un rivelatore.

Inoltre è necessario che il rivelatore funzioni sempre in modalità lineare, e mai in modalità Geiger; per fare ciò bisogna abbassare la V_{bias} applicata. Per ottenere questo, nell'esperimento riportato, i rivelatori sono stati illuminati con un'altra sorgente sovrapposta a quella di segnale; questa invia una energia dell'ordine del μW al rivelatore, riscaldandolo, e quindi abbassandone il voltaggio. Una soluzione proposta a ciò è un controllo sulla potenza in entrata nel rivelatore. Il risultato di questo controllo, però, dovrebbe anch'esso essere computato nello studio della sicurezza dei protocolli.

Si è mostrato qui un esempio di attacco ad un dispositivo pratico di QKD, fondato sulle debolezze dell'elettronica. Questo tipo di attacco può essere risolto con ulteriori strumenti di controllo, ma altri attacchi potrebbero essere poi ideati. Il lato della non idealità dell'elettronica è dunque un punto debole della attuale QKD. Recentemente è stata proposta una soluzione a questo problema, che permette di avere sicurezza incondizionata anche nel caso in cui i rivelatori siano totalmente inaffidabili, come nell'esperimento precedente. Questa soluzione è la *measurement-device-independent QKD*.

Capitolo 3

Measurement-Device-Independent QKD

In questo capitolo introduciamo la *measurement-device-independent QKD*, il cui scopo principale è quello di rimuovere tutte le vulnerabilità del sistema al lato rivelatore (es: 2.2).

Il funzionamento di questa procedura si può riassumere in questo modo: sia Alice che Bob preparano fotoni come per un protocollo *BB84* (1.2.1 , chiameremo le due basi *rettilinea* e *diagonale*) e li inviano a Charlie, un ripetore posto al centro, che effettua su ciascuna coppia di fotoni una misura di stato di Bell. Finita la trasmissione, Charlie annuncia pubblicamente quando ha ottenuto una misura positiva e dichiara il risultato. Alice e Bob prima eliminano i dati per i quali Charlie non ha ottenuto un risultato positivo, effettuano se necessario il *sifting*, ed infine per correlare le due stringhe attuano una fase di *bit-flip* come illustrato in tabella 3.1. Alice e Bob procedono dunque con la post-elaborazione ed ottengono la chiave segreta.

Il ruolo di Charlie consiste nel proiettare la coppia di fotoni di Alice e Bob in uno stato di Bell. Per fare questo utilizza un setup come in figura 3.1. La misura di uno stato di Bell ha successo solo se esattamente due rivelatori cliccano. In particolare le combinazioni $D_{1H} - D_{2V}$ e $D_{1V} - D_{2H}$ corrispondono allo stato di singoletto $|\psi^-\rangle$, mentre $D_{1H} - D_{1V}$ e $D_{2H} - D_{2V}$ corrispondono allo stato di tripletto $|\psi^+\rangle$, dove H, V sono gli autostati della base rettilinea.

Quanto illustrato è reso possibile dall'*effetto HOM*: quando due fotoni uguali entrano in uno *beam-splitter (BS)* 50:50 essi usciranno sempre assieme nello stesso ramo; inoltre se i due fotoni avevano stati di polarizzazione ortogonali ed escono nello stesso ramo, allora raggiungeranno lo stesso rivelatore (dopo essere passati in un *polarizing-beam-splitter (PBS)*.

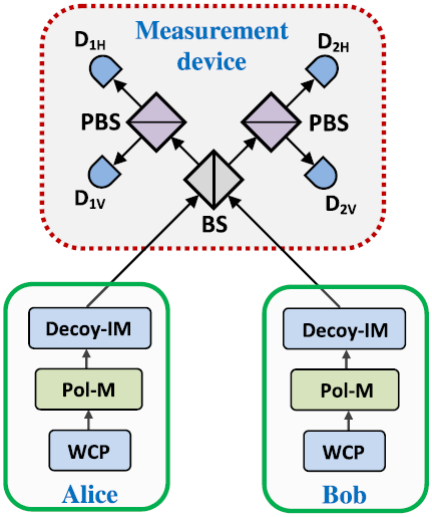
Nella realizzazione pratica è però complicato produrre due fotoni indistinguibili da due differenti Laser, ed ottenere una interferenza di HOM stabile.

Si prova ad osservare il fenomeno [4] con due Laser di diversi produttori, uno (S1) a lunghezza d'onda fissa $1550nm$ e l'altro (S2) a lunghezza d'onda variabile, entrambi con larghezza in frequenza minore di $1MHz$. La frequenza di S2 può essere variata a passi di $0.1pm$ (circa $13MHz$ a $1550nm$). Il ritardo tra gli impulsi dei due laser è gestito alla risoluzione del ps. Lo spettro degli impulsi, in uscita dai modulatori di intensità, ha larghezza di banda pari a circa $5GHz$, molto maggiore dell'errore sulla frequenza centrale, mantenuto minore di $30MHz$. Si producono quindi due fotoni indistinguibili che dovrebbero interferire.

Tabella 3.1: Fase di bit-flip per il protocollo di MDI-QKD. Uno tra Alice e Bob esegue i bit flip dei suoi dati secondo questo schema.

Alice e Bob	Charlie Output $\|\psi^-\rangle$	Charlie Output $\|\psi^+\rangle$
Base rettilinea	bit flip	bit flip
Base diagonale	bit flip	NO bit flip

Figura 3.1: Tipico setup per un protocollo MDI-QKD. Legenda: WCP impulsi coerenti attenuati (Laser); Pol-M modulatore di polarizzazione; Decoy-IM modulatore di intensità per produrre stati decoy; BS beam splitter 50:50; PBS beam splitter polarizzatore, che proietta i fotoni negli stati H e V della base rettilinea; Ds rivelatori.



La misura dell'interferenza si fa, dopo un *beam-splitter*, con due rivelatori di singolo fotone (SPD). L'intensità dell'impulso è impostata pari a $\mu = 0.1$. Si effettuano misure di coincidenza per diversi intervalli di ritardo tra i due segnali, ed il risultato è esposto in figura 3.2. Si osserva che la buca è altamente visibile, anche se non va a zero come previsto dalla teoria, e dunque l'effetto è utilizzabile a scopi pratici.

In un setup sperimentale come da figura 3.1, Alice e Bob possono calcolare con tecniche statistiche il *gain* Q (probabilità che la misura di Charlie sia positiva) e il *QBER* E, e si può ricavare il tasso di produzione della *secure key* [4]

$$R = Q^{1,1}_{rect}[1 - H(e^{1,1}_{diag})] - Q_{rect} f(E_{rect}) H(E_{rect}) \tag{3.1}$$

dove: $Q^{i,j}$ e $e^{i,j}$ sono il gain e il QBER di un segnale dove Alice e Bob inviano rispettivamente i e j fotoni, $Q = \sum_{n,m} Q^{n,m}$, $E = \sum_{n,m} Q^{n,m} e^{n,m}/Q$, $f(\cdot)$ dà una stima dell'efficienza della correzione errori, $H(\cdot)$ è l'entropia binaria di Shannon. A pedice è stato indicato l'insieme su cui è stimato il parametro: dei fotoni prodotti in base rettilinea oppure diagonale.

Una simulazione del tasso di produzione della chiave è stata fatta, considerando una fibra ottica con perdita di segnale $\alpha = 0.2 dB/km$ ed efficienza $f(E_{rect}) = 1.16$. I risultati (in figura 3.3) mostrano che il *raw key rate* è comparabile a quello di altre tecniche e che l'apparato può sopportare un alto rumore, permettendo di trasmettere a distanze di $200 km$ (se Charlie è posto al centro tra Alice e Bob).

3.1 Realizzazioni sperimentali

Proponiamo di seguito due esperimenti di *MDI-QKD* di recente pubblicazione.

Esperimento 1

Esponiamo qui la prima implementazione pratica di MDI-QKD con codifica nella polarizzazione, prodotta con dispositivi commerciali [5]. L'utilizzo della polarizzazione è preferito ad altre

Figura 3.2: Effetto HOM. Viene definita la *normalized coincedence rate* come $C = P_C/(P_1P_2)$ dove P_1 e P_2 sono la probabilità di rivelazione di SPD_1 e SPD_2, e P_C la probabilità di avere un click simultaneo entro $2ns$ di SPD_1 e SPD_2

.

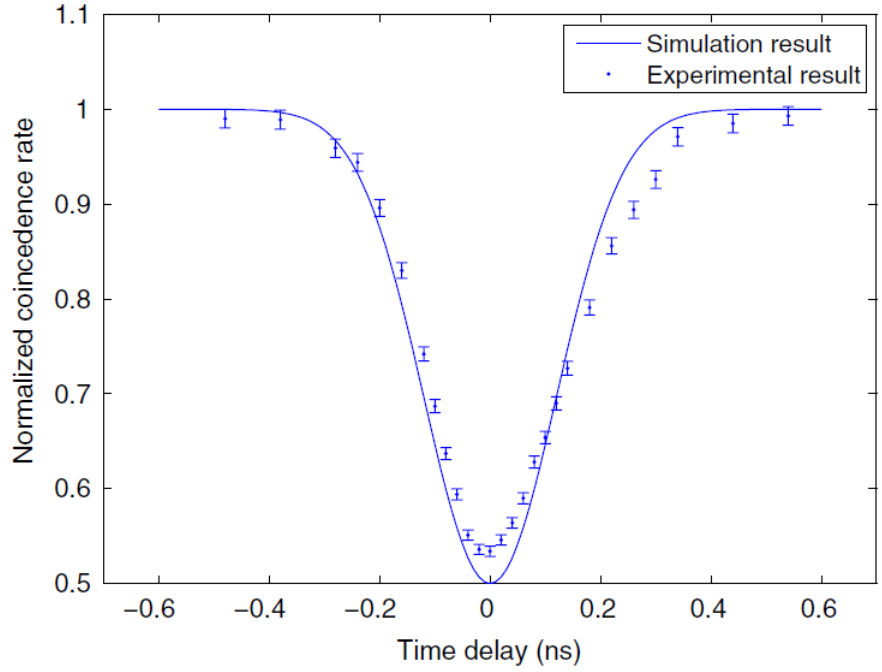


Figura 3.3: Tasso di produzione della chiave. In verde la simulazione del tasso di produzione dato dalla equazione 3.1. I parametri utilizzati: perdita del canale $\alpha = 0.2dB/km$, errore per il disallineamento del sistema 1.5%, efficienza del sistema di rivelazione 14.5%, tasso di dark count 6.02×10^{-6}. In rosso, per confronto, i risultati per un protocollo EB.

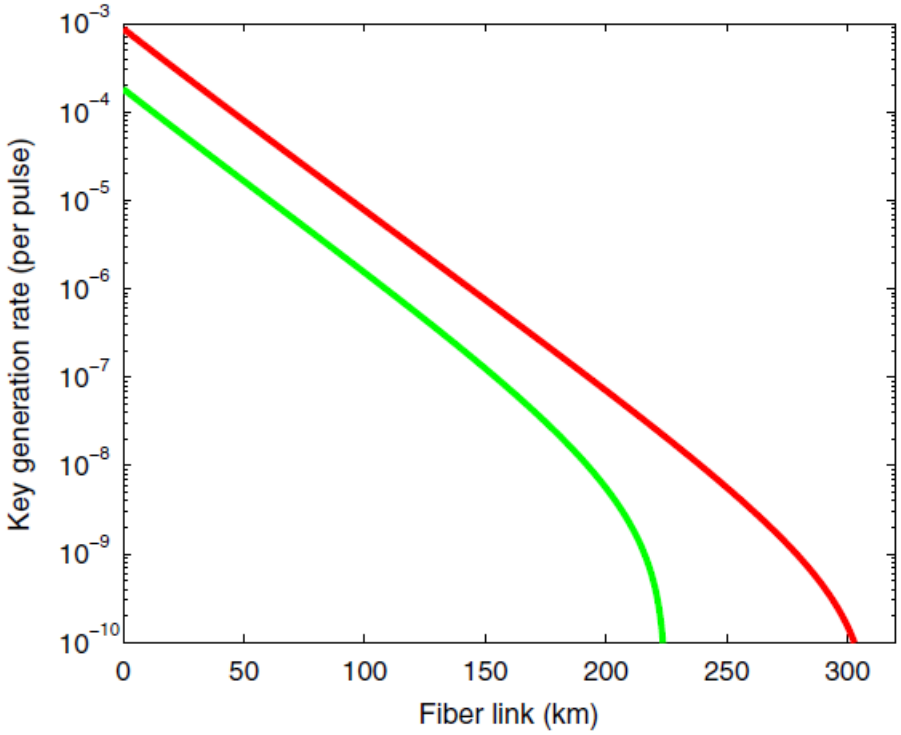
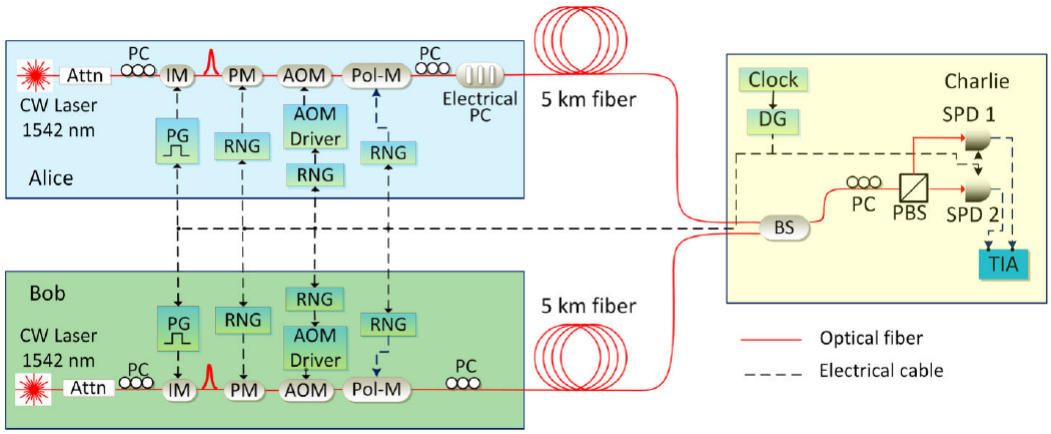


Figura 3.4: Apparato sperimentale.Legenda: Attn attenuatori; IM modulatore di intensità; PM modulatore di fase; AOM modulatore ottico-acustico; Pol-M modulatore di polarizzazione; PC controllo di polarizzazione; PG generatore impulsi elettrici; RNG generatori di numeri casuali; BS beam splitter; PBS beam splitter polarizzatore; SPDs rivelatori di singolo fotone; TIA analizzatore di intervallo temporale; DG delay generator.



codifiche, come fase e time-bin, per la maggiore semplicità di implementazione, fondamentale per uno sviluppo commerciale.

Questa dimostrazione sperimentale è stata effettuata con randomizzazione attiva di fase su $10km$ si fibra ottica. Valore dei bit, basi e intensità del impulso Laser sono scelti casualmente.

I parametri sono ottimizzati con una simulazione numerica: intensità del segnale $\mu = 0.3$ e intensità dei due *decoy-state*: $\nu = 0.1$, $\omega = 0.01$. Gli impulsi sono inviati nel rapporto $4 : 9 : 7$ rispettivamente μ, ν, ω.

L'apparato sperimentale utilizzato è descritto in figura 3.4. Alice e Bob possiedono ciascuno un Laser a frequenza fissa $1542nm$, attenuato da un *modulatore di intensità* (IM) al $LiNbO_3$ per produrre impulsi coerenti ad una frequenza di $500kHz$. La fase è modulata da un *modulatore di fase* (PM) in modo casuale nell'intervallp $[0, 2\pi]$. Gli stati di segnale e *decoy* sono prodotti da un *modulatore ottico-acustico* (AOM). Infine i bit sono codificati da un *modulatore di polarizzazione* (Pol-M). Tutti i modulatori sono gestiti indipendentemente da generatori di numeri casuali. Il tutto è sincronizzato da un *delay generator* (DG), posto nel setup di Charlie, attraverso un segnale elettrico su una linea classica. In futuro il segnale di sincronizzazione potrebbe essere inviato anch'esso nella fibra.

Per avere stati correlati le basi di Alice e Bob devono essere allineate. Come prima operazione entrambi allineano la loro base rettilinea a quella del *beam-splitter* di Charlie. Successivamente Alice allinea la base diagonale con un dispositivo elettrico per il controllo della polarizzazione (Electrical PC). L'errore sull'allineamento finale è stimato in circa l'1%. La polarizzazione resta stabile durante l'esperimento per più di un'ora, e ogni ora viene rieffettuato l'allineamento.

Un'ulteriore necessità del sistema è che Alice e Bob producano fotoni indistinguibili, per avere interferenza di HOM. Questo è reso possibile dall'utilizzo di Laser identici a lunghezza d'onda stabilizzata a circa $1542.38nm$. Si ha garantita una differenza di frequenza tra Alice e Bob minore di $10MHz$, mentre la larghezza ($FWHM$) dell'impulso è molto maggiore, attorno a $1GHz$; lo spettro è quindi sovrapposto ottimamente. Per quanto riguarda la sovrapposizione temporale di arrivo dei due fotoni, essa è gestita dal DG, con una risoluzione di $50ps$, mentre il tempo di misura dell'elettronica è circa $100ps$. Si ottiene quindi un ottimo overlap tra i due fotoni, sia per quanto riguarda lo spettro che il tempo.

Tabella 3.2: Valori sperimentali di gain (Q) e QBER (E), per gli impulsi di segnale (intensità μ). Gli errori rappresentano 3 deviazioni standard.

	base rettilinea	base circolare
$Q_{\mu\mu} \times 10^4$	0.466+-0.005	0.903+-0.006
$E_{\mu\mu}$	0.018+-0.001	0.262+-0.004

Tabella 3.3: Parametri sperimentali, utilizzati per il calcolo del key rate.

q	p_{11}	$Y_{1,1}^{Z,I}$	$e_{1,1}^{X,S}$	f
0.011	0.0494	$4.1 \times 10^{-}4$	0.151	1.16

La comunicazione sul canale quantistico avviene con il procedimento standard della MDI-QKD (descritto ad inizio capitolo, vedi figura 3.1). In questo caso però sono posti rivelatori solo su un ramo del beam-splitter, di conseguenza viene riconosciuto solo lo stato di tripletto di Bell $|\psi^+\rangle$.

Vengono inviati $N = 1.69 \cdot 10^{11}$ impulsi, si effettua il sifting e si calcolano *gain* e *QBER*. I cui valori, per gli impulsi di segnale (μ), sono riportati in tabella 3.2. Si osserva che il QBER è molto piccolo nella base rettilinea, mentre maggiore in quella circolare; questo era atteso in quanto il primo sarebbe idealmente nullo, e dovuto in questo caso all'errore sull'allineamento delle basi, mentre il secondo è maggiore a causa dell'esistenza di impulsi a più fotoni.

Si trova il *secret key rate* [5]

$$R \geq q\{p_{11}Y_{1,1}^{Z,I}[1 - H(e_{1,1}^{X,S})] - Q_{\mu\mu}^{Z} f(E_{\mu\mu}^{Z}) H(E_{\mu\mu}^{Z})\} \tag{3.2}$$

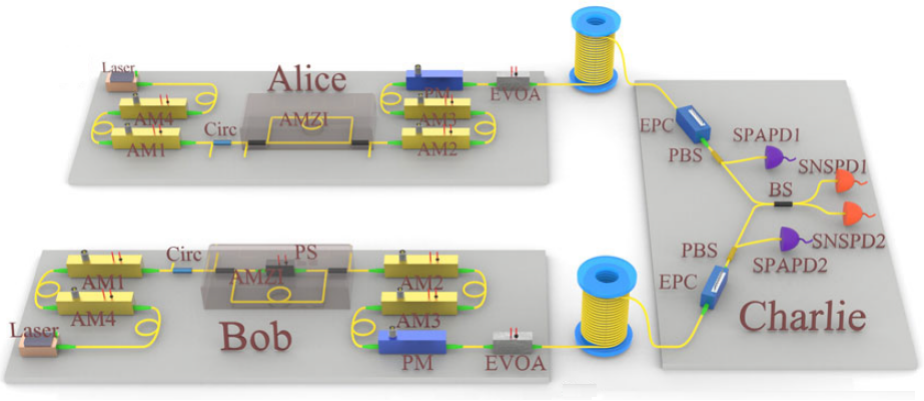
dove q è la probabilità che sia Alice che Bob inviino un segnale nella base rettilinea; $p_{1,1,} = \mu^2 e^{-2\mu}$ è la probabilità che entrambi mandino un segnale di singolo fotone data l'intensità μ; $f(\cdot) > 1$ è l'efficienza della correzione degli errori; $H(\cdot)$ l'entropia binaria di Shannon; $Y_{1,1}^{Z,I}$ e $e_{1,1}^{X,S}$ indicano, per uno stato a singolo fotone, rispettivamente il limite inferiore dell'affidabilità in base rettilinea e il limite superiore del QBER in base diagonale. Questi due parametri sono entrambi stimati con metodi analitici sugli stati *decoy* (vedi sez. 2.1, eq. 2.9 e 2.10). Gli indici ad apice indicano la base: Z rettilinea, X diagonale, W entrambe; gli indici a pedice indicano: se numerici il numero di fotoni dell'impulso, se lettere greche il tipo di segnale: μ, ν o ω.

Sulla base dei parametri risultati dall'esperimento (vedi tabella 3.3) si stima la lunghezza minima della chiave sicura estratta: $L = NR \simeq 1600bit$.

Il tasso di produzione ottenuto non è molto elevato, ma può essere migliorato con semplici accorgimenti. Una maggiore frequenza di produzione dei segnali migliorerebbe le stime di $Y_{1,1}^{Z,I}$ e $e_{1,1}^{X,S}$, inoltre, utilizzando un maggior numero di dati, si potrebbe diminuire la frazione di stati *decoy* per aumentare quella di stati di segnale. Si osserva che utilizzando migliori rivelatori commerciali, con frequenza di rivelazione fino a $100MHz$, si potrebbe ottenere un rate di generazione della chiave pari a $1kbps$ a distanze di $50km$ su fibra; poi l'utilizzo di quattro rivelatori, anziché due, quadruplicherebbe la velocità.

Si è quindi riusciti a riprodurre un esperimento pratico di MDI-QKD con l'utilizzo di strumenti commerciali prefabbricati, ottenendo dunque un dispositivo di QKD di facile produzione ed immune ad attacchi al rivelatore.

Figura 3.5: Apparato sperimentale per la trasmissione del segnale. Legenda: AM modulatori di intensità; AMZI interferometro asimmetrico Mach-Zender; PM modulatore di fase; EPC controllo di polarizzazione elettrico; PBS beam splitter polarizzatore; SPAPD avalanche photodiode a singolo fotone; BS beam splitter; SNSPD rivelatore di singolo fotone a nanofili superconduttori.



Esperimento 2

Una seconda realizzazione [6] si propone di creare un apparato di MDI-QKD con performance migliori dei precedenti esperimenti, per raggiungere una *key-rate* paragonabile a quella di altri metodi su lunghe distanze. In particolare si riuscirà a produrre una trasmissione a $200km$ con un aumento del tasso di produzione della chiave di 3 ordini di grandezza.

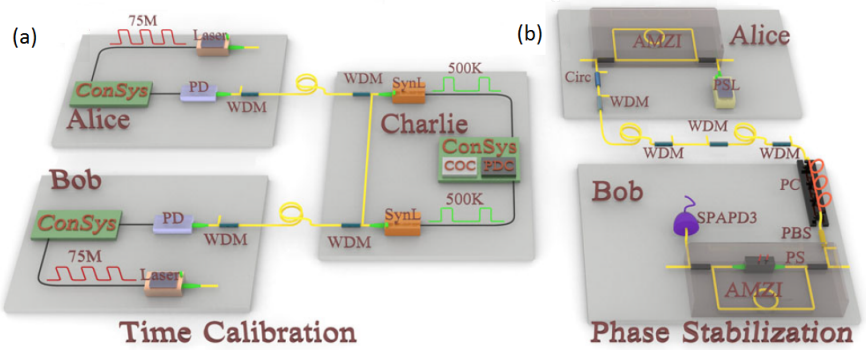
L'apparato sperimentale è mostrato in figura 3.5. I Laser di Alice e Bob, di lunghezza d'onda $1550nm$, vengono modulati per creare treni di impulsi di larghezza $2.5ns$ con una frequenza di $75MHz$. L'intensità è modulata in tre modi, per l'utilizzo di due stati *decoy*, con valori $\mu = 0.4$, $\nu = 0.07$, $\omega = 0$ (ossia stato di *vuoto*) e rapporto di produzione $33 : 45 : 22$; parametri ottimizzati per l'utilizzo su $200km$ di fibra. Si utilizza uno schema di codifica a fase e *time-bin*, prodotto con un *interferometro asimmetrico Mach-Zehnder* (AMZI), tre *modulatori di ampiezza* (AM) e un *modulatore di fase* (PM). Il AMZI divide l'impulso in due bin distanti $6.5ns$. La prima base (Z) viene codificata in time-bin da AM1 e AM2, la seconda (X) in fase relativa (tra due impulsi successivi) dal PM. AM4 viene utilizzato per normalizzare il numero di fotoni per ciascuna base.

I segnali prodotti vengono inviati attraverso una fibra ottica, di lunghezza tra $25km$ e $100km$ per lato, a Charlie che effettua la misura dello stato di Bell. L'aspetto critico dell'apparato consiste ancora nel produrre una buona interferenza tra i due fotoni.

La sincronizzazione temporale è eseguita su una seconda fibra ottica tra Alice, Bob e Charlie (figura 3.6). Alice e Bob inviano impulsi, con un secondo Laser, a Charlie con un periodo indicato da Charlie stesso. Charlie misura la differenza del tempo di arrivo tra i due fotoni, e modifica il segnale di sincronizzazione in modo da riceverli contemporaneamente. La calibrazione ha una precisione di $20ps$, molto minore della larghezza dei segnali ($2.5ns$). Questo permetterà di effettuare la codifica a time-bin.

Per garantire la sovrapposizione degli spettri, i due Laser utilizzati hanno caratteristiche spettrali (*FWHM* e lunghezza d'onda centrale) quasi uguali. Inoltre si misura la frequenza con un *analizzatore dello spettro ottico* (OSA), con precisione $1pm$. In seguito si eguagliano le due lunghezze d'onda, modificando la temperatura dei laser, con precisione di circa $0.5pm$. Come risultato la differenza tra le due lunghezze d'onda sarà molto minore della FWHM del segnale,

Figura 3.6: Apparato sperimentale per la calibrazione. **a**, calibrazione temporale. Legenda: ConSys sistema di controllo; PD rivelatore fotoelettrico; WDM multiplexer a divisioni in lunghezza d'onda; SynL Laser di sincronizzazione; COC circuito a cristallo oscillante; PDC delay chip programmabile. **b**, stabilizzazione della fase. Legenda: AMZI interferometro asimmetrico Mach-Zender; PC controllo di polarizzazione; PBS beam splitter polarizzatore; PS modificatore di fase; SPAPS avalanche photodiode a singolo fotone.



misurata in circa $4pm$ con risoluzione $0.06pm$. Infine la polarizzazione viene stabilizzata in *real-time* con un *controllo elettrico di polarizzazione*. Questo permette di inviare un segnale a Charlie con una fluttuazione di potenza inferiore al 3%.

La codifica in fase richiede una ulteriore calibrazione tra Alice e Bob: la fase di riferimento, ossia quella relativa tra i due bracci del AMZI, può cambiare nel tempo a causa dello stress e di fluttuazioni nella temperatura. Per stabilizzarla Alice invia un segnale da un terzo laser (PSL) attraverso gli AMZI proprio e di Bob, collegati da una linea ottica diretta. Bob controlla la potenza in uscita da un braccio del suo AMZI e tiene calibrata la fase con un *phase shifter* (vedi figura 3.6).

Le calibrazioni descritte permettono di avere un segnale stabile per la comunicazione, che può rimanere operativo senza aggiustamenti per oltre 1 giorno.

Si trova il *secure key rate* [6]

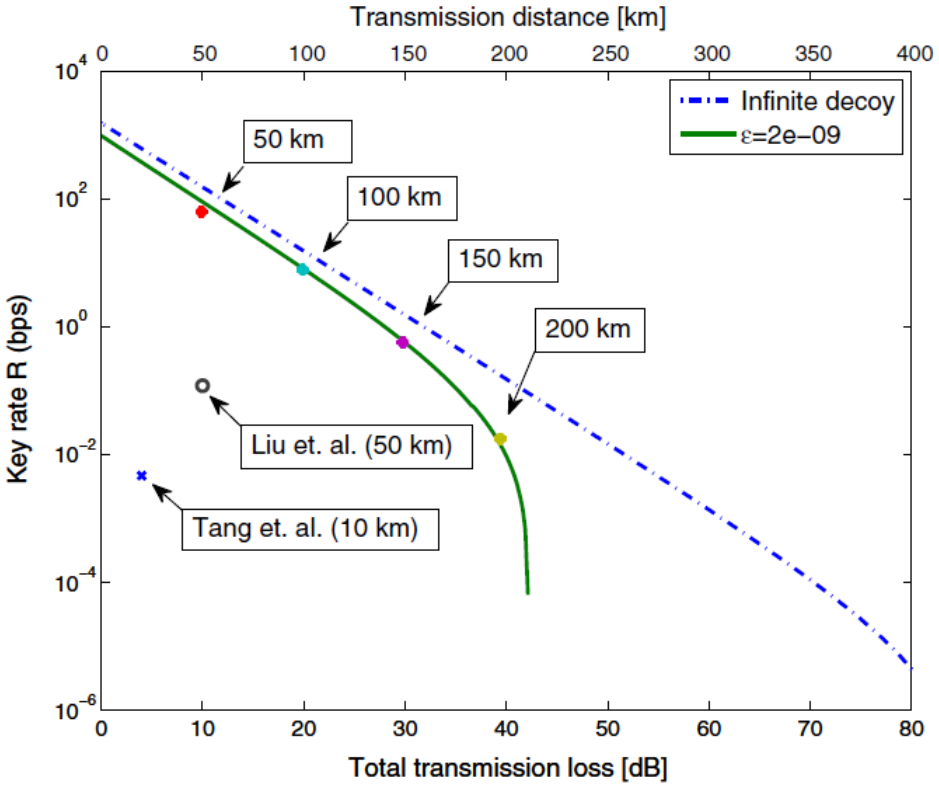
$$R \geq Q_{1,1}^{\mu\mu}[1 - H(e_{1,1}^{\mu\mu})] - Q^{\mu\mu} f H(E^{\mu\mu}) \tag{3.3}$$

dove $Q^{\mu\mu}$ e $E^{\mu\mu}$ sono il gain e il QBER quando vengono prodotti due impulsi di segnale; $Q_{1,1}^{\mu\mu}$ e $e_{1,1}^{\mu\mu}$ sono i limiti di gain e QBER, per segnali a singolo fotone, dati dall'analisi sugli stati decoy (vedi sez. 2.1, eq. 2.11 e 2.12); $H(\cdot)$ l'entropia binaria di Shannon ed f l'efficienza della correzione errori, stimata in $f = 1.16$.

L'apparato è stato messo in funzione per 130 ore, utilizzando fibra ottica di lunghezze 50, 100, 150 e 200 km. I risultati sono mostrati in figura 3.7. Ad una distanza di $200km$ è stato raggiunto un tasso di produzione di $0.018bit/s$ della chiave segreta.

Si è quindi dimostrata la possibilità della realizzazione di dispositivi MDI-QKD su lunghe distanze, con una buona efficienza. La velocità di produzione potrà essere ulteriormente migliorata attraverso l'utilizzo di frequenze di clock maggiori e rivelatori con una migliore efficienza.

Figura 3.7: Key rate dell'esperimento e simulazioni. I quattro punti corrispondono ai dati sperimentali per 50km ($9.9dB$), 100km ($19.9dB$), 150km ($29.8dB$), 200km ($39.6dB$). La linea continua mostra i risultati di una simulazione con i parametri dell'esperimento. Quella tratteggiata una simulazione ottimale con infiniti stati decoy. I restanti due punti sono riferiti a precedenti esperimenti, in particolare *Tang et. al.* è quello descritto in *Esperimento 1* [5].



Bibliografia

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lűtkenhaus, M. Peev, *The security of practical quantum key distribution*, Reviews of Modern Physics **345**, 1301-1350 (2009).

[2] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Practical decoy state for quantum key distribution*, Physical Review A **72**, 012326 (2005).

[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, *Hacking commercial quantum cryptographi system by tailored bright illumination*, Nature Photonics **4**, 686-689 (2010).

[4] H.-K. Lo, M. Curty, B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Physical Review Letters **108**, 130503 (2012).

[5] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.-K. Lo, *Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution*, Physical Review Letters **112**, 190503 (2014).

[6] Y.-L. Tang, H.-L. Yin, S.-J. Cheng, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, J.-W. Pan, *Measurement-Device-Independent Quantum Key Distribution over 200 km*, Physical Review Letters **113**, 190501 (2014).